Пример графической подписи

4. Выполнен анализ экономической эффективности проекта.

Дальнейшими направлениями работы являются: оценка уровня защищенности СЭД и локализация узких мест в системе защиты СЭД, выработка рекомендаций по повышению эффективности существующих механизмов безопасности СЭД.

РАЗРАБОТКА DLP-СИСТЕМЫ С УЧЕТОМ МОБИЛЬНЫХ УСТРОЙСТВ НА ОС ANDROID

А. М. Кофанов, И. А. Плетнинцев
(Курган, КГУ, kofanov.alexandr@mail.ru; payne-xl@mail.ru)

Введение

Необходимость защиты от внутренних угроз была очевидна на всех этапах развития средств информационной безопасности. Однако первоначально внешние угрозы считались более опасными. В последние годы на внутренние угрозы стали обращать больше внимания, что выражается в росте популярности DLP-систем [1]. С недавнего времени на замену стационарным компьютерам при-

ходят мобильные устройства: планшеты, смартфоны. В данной работе предложен взгляд авторов на проблему развертки DLP-системы на ОС Android.

Общее описание

Для начала следует определиться с тем, что мы будем подразумевать под термином DLP-система. Термин DLP – Data Loss Prevention (или Data Leak Prevention, защита от утечек данных), предложен в 2005 г. В качестве русского аналога термина было принято словосочетание «системы защиты конфиденциальных данных от внутренних угроз». При этом под внутренними угрозами понимаются злоупотребления (намеренные или случайные) со стороны сотрудников организации, имеющих легальные права доступа к соответствующим данным, своими полномочиями [2].

Наиболее стройные и непротиворечивые критерии принадлежности к DLP-системам были выдвинуты исследовательским агентством Forrester Research в ходе их ежегодного исследования данного рынка. Они предложили четыре критерия, в соответствии с которыми систему можно отнести к классу DLP:

1. Многоканальность. Система должна быть способна осуществлять мониторинг нескольких возможных каналов утечки данных. В сетевом окружении это как минимум e-mail, Web и IM, а не только сканирование почтового трафика или активности базы данных. На рабочей станции пользователя также необходим мониторинг файловых операций, работы с буфером обмена данными.

2. Унифицированный менеджмент. Система должна обладать унифицированными средствами управления политикой информационной безопасности, анализом и отчетами о событиях по всем каналам мониторинга.

3. Активная защита. Система должна не только обнаруживать факты нарушения политики безопасности, но и при необходимости принуждать к ее соблюдению. К примеру, блокировать подозрительные сообщения.

4. Учет как содержания, так и контекста. В процессе классификации документов, циркулирующих по возможным каналам утеч-

ки данных, необходимо учитывать не только ключевые слова и регулярные выражения, встречающиеся в этом документе, но и его общее содержание. Система также должна учитывать и контекст: тип приложения, протокол, активность, отправителя, адресат и т. п. [2].

Защита конфиденциальной информации осуществляется DLP-системой при помощи использования следующих основных функций:

- фильтрация трафика по всем каналам передачи данных;
- глубокий анализ трафика на уровне контента и контекста.

Защита конфиденциальной информации в DLP-системе осуществляется на трех уровнях: Data-in-Motion, Data-at-Rest, Data-in-Use.

К уровню Data-in-Motion относятся данные, передаваемые по сетевым каналам:

- Web (HTTP/HTTPS протоколы);
- Интернет-мессенджеры (ICQ, QIP, Skype, MSN и т. д.);
- корпоративная и личная почта (POP3, SMTP, IMAP и т. д.);
- беспроводные системы (Wi-Fi, Bluetooth, 3G и т. д.);
- FTP – соединения.

К уровню Data-at-Rest относятся данные, статично хранящиеся:

- на серверах;
- рабочих станциях;
- ноутбуках;
- системах хранения данных (СХД).

К уровню Data-in-Use относятся данные, используемые на рабочих станциях.

Меры, направленные на предотвращение утечек информации, состоят из двух основных частей: организационных и технических.

Организационные меры

Защита конфиденциальной информации включает в себя организационные меры по поиску и классификации имеющихся в компании данных. В процессе классификации данные разделяются на 3 категории:

- секретная информация;
- информация для служебного пользования;
- общедоступная информация.

В DLP-системах конфиденциальная информация может определяться по ряду различных признаков, а также различными способами, например:

- лингвистический анализ информации;
- статистический анализ информации;
- регулярные выражения (шаблоны);
- метод цифровых отпечатков и т. д.

После того как информация найдена, сгруппирована и систематизирована, следует вторая организационная часть – техническая.

Технические меры

Защита конфиденциальной информации при помощи технических мер основана на использовании функционала и технологий системы по защите данных от утечек. В состав DLP-системы входят два типа модулей: хост модуль и сетевой модуль.

Хост модули устанавливаются на рабочие станции пользователей и обеспечивают контроль действий, производимых пользователем в отношении классифицированных данных (конфиденциальной информации). Кроме того, модуль хоста позволяет отслеживать активность пользователя по различным параметрам, например время, проведенное в Интернете, запускаемые приложения, процессы и пути перемещения данных и т. д.

Сетевой модуль осуществляет анализ передаваемой по сети информации и контролирует трафик выходящей за пределы защищаемой информационной системы. В случае обнаружения в передаваемом трафике конфиденциальной информации сетевой модуль пресекает передачу данных [3].

Построение DLP-системы на мобильной платформе

Описанные выше общие требования DLP-систем не учитывают специфику мобильных устройств. К ним можно отнести:

- Новую, в том числе с точки зрения безопасности, архитектуру, отличную от привычной Intel × 86.
- Высокую скорость перехода мобильных устройств из одной среды передачи информации в другую.

• Наличие отдельного класса специализированных ОС для мобильных устройств. Сегодня существует большое разнообразие как видов, так и подвидов таких ОС. Они часто обновляются, причем нередко обновления включают изменения ядра (например, ОС Android).

• Мобильность, причем не просто возможность физического переноса прибора. Современная мобильность подразумевает автономность и свободу от ограничений по времени, месту, способу доступа к необходимой информации, средствам связи и приложениям.

Следующий план отображает
наше видение разработки DLP-системы:

1. DLP-система должна состоять из следующих модулей:

1.1. Хост модуля.

1.2. Сетевого модуля.

1.3. Управляющего модуля, который осуществляет политику безопасности, заданную администратором безопасности при внедрении DLP-системы и в процессе ее жизненного цикла.

1.4. Файловое хранилище осуществляет хранение данных в зашифрованном виде.

2. Любому файлу, содержащему конфиденциальную информацию, должен быть присвоен гриф. Определены три грифа: секретные, конфиденциальные и общедоступные данные. Гриф присваиваются вручную при создании файла. Это необходимо для реализации технологии детектирования данных, т. е. поиска в файлах меток грифа.

3. Файлы, содержащие конфиденциальную информацию, должны храниться на сервере в зашифрованном виде.

4. Должна быть реализована функция сохранения файлов, содержащих конфиденциальную информацию на устройстве. Данное решение необходимо для работы с конфиденциальными документами в командировках.

5. В управляющем модуле должны быть реализованы следующие функции:

5.1. Идентификации и аутентификации сотрудников и устройств.

5.2. Управления идентификаторами: создание, присвоение, уничтожение;

5.3. Управления средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации [4].

6. При попытке авторизации пользователя сервер должен организовать защищенный канал передачи данных. И дальнейшая работа с сервером идет по этому защищенному каналу.

7. Анализ трафика должен представлять собой механизмы поиска конфиденциальных данных в потоке пакетов данных.

8. Анализ трафика должен быть реализован в двух режимах: работа через защищенный канал (ведомственная сеть передачи данных) и работа через открытый канал данных (Интернет).

8.1. При работе в ведомственной сети функцию анализа трафика берет на себя сервер.

8.2. При работе в сети Интернет анализ трафика осуществляется непосредственно на устройстве.

9. Анализ действий пользователя должен включать в себя попытки предотвращения:

9.1. Копирования конфиденциальной информации из документа с ограниченным доступом в документ с открытым доступом.

9.2. Передачи файлов через Bluetooth, NFC и другие каналы.

9.3. Копирования конфиденциальных данных на съемные носители.

10. Должны быть реализованы сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения, а также защита информации о событиях безопасности.

11. При обнаружении утечки информации необходимо:

11.1. Задокументировать событие.

11.2. Попытаться предотвратить утечку.

11.3. Использовать этот опыт для предотвращения подобных утечек в будущем.

12. Доступ к журналу с зарегистрированным событиям безопасности возможен только в следующих случаях:

12.1. Обнаружение утечки конфиденциальной информации.

12.2. Сбой системы.

12.3. При попытке несанкционированного доступа к конфиденциальным данным.

Тот факт, что устройство на Android является мобильным, привносит новые проблемы, которых лишены стационарные компьютеры. В связи с этим имеют место разработки нового модуля DLP-системы. В данной работе сформулированы общие требования при разработке DLP-системы для мобильных устройств.

Библиографические ссылки

1. Википедия: свободная энциклопедия [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B4%D0%BE%D1%82%D0%B2%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%B8%D0%B5_%D1%83%D1%82%D0%B5%D1%87%D0%B5%D0%BA_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8, свободный.

2. PCWEEK Безопасность [Электронный ресурс]. Режим доступа: http://www.pcweek.ru/security/article/detail.php?ID=109716, свободный.

3. Pointlane Информационная Безопасность [Электронный ресурс]. Режим доступа: http://www.pointlane.ru/solutions/dlp/, свободный.

4. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21.

МЕТОД ОЦЕНКИ УЯЗВИМОСТЕЙ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ АСУ ТП

А. И. Кураленко, А. С. Яценко
(Томск, ТУСУР, alkur@sibmail.com; yas@ttfoms.tomsk.ru)

Автоматизированные системы управления техническим процессом прочно вошли в нашу жизнь, на сегодняшний день они внедрены повсеместно, где необходима автоматизация. Для таких объек-